

REMARKS/ARGUMENTS

Status

No claim has been cancelled by the present amendment. Claims 1-57, including independent claims 1, 29 and 45, will remain for further consideration.

More Clearly Defined

The claims in this application have been revised to voluntarily further clarify Applicant's unique invention. Applicant maintains that the claims as filed were patentable over the art of record. However, to expedite issuance of this application, reconsideration of the claims in light of the amendments and for the following reasons is respectfully requested.

Claim History

The Examiner rejected claims 1-4, 6-16, 21-36, 40-51 and 53-57 under 35 U.S.C. § 103 over Everingham in view of Walker. The Examiner rejected claim 5 under 35 U.S.C. § 103 over Everingham in view of Walker and in further view of Bouchard. The Examiner rejected claims 17-20, 36-39 and 52 under 35 U.S.C. § 103 over Everingham in view of Walker and in further view of Geiger et al. This rejection is respectfully traversed.

The present invention is to a method of ensuring that a document remains encrypted whether or not a recipient has a key. An important part of this goal is to encrypt the document while the document is sent between the sender and the system that will store the document pending delivery to a user. When the user has a public key, the document can be stored right away using the public key. When the user does not have a

public key, or it is unavailable to the sender, an escrow key is used to temporarily encrypt the file. The recipient is then requested to generate or supply the key. The document can then be encrypted with the recipient's key to provide end to end encryption of the document between the sender and the recipient without requiring that the sender hold the document until the recipient provides a key. This is especially important where as in the current invention, multiple recipients of the message are included.

In contrast, the patent to Everingham shows a standard electronic document routing system without encryption or escrow encryption. The published application is to a method of encrypting data by retrieving a locking key stored in a database. Unlike the present invention, Walker does not disclose an escrow key. Walker merely shows the expedient of assigning a public key to a recipient if the recipient does not currently have a public key. This does not serve the same function as the escrow key, because encrypting the document is meaningless if the recipient is also sent the unlocking key. Additionally, the claims require that the escrow key is not the same as the recipient's public key. Walker does not teach such a system. Claim 29 as provided previously and in its current form require "said key is set equal to a generated escrow encryption key not equal to the recipient's public key." However, in Walker since the recipient's public key is the only key generated, the key that the Examiner is calling a "escrow key" is merely the public key, so therefore they must *de facto* be equal. Claim 45 as amended also requires that "wherein the recipient's public key is not equal to said escrow encryption key." Claim 1 as amended also requires "an escrow encryption key not equal to the recipient's public key and not equal to the sender's private key." Claim 1 also further requires that the escrow unencryption key for unlocking said escrow encryption key is not made available to said recipient. The escrow encryption key in main provides for internal encryption of the file

using a key that is unavailable to other parties so that the document encrypted cannot be altered or viewed. Providing the private key stored with the document may not provide such security against an internal party such as the system administrator from violating the security of the document.

Additionally, there is no motivation to combine. Walker at best relates to single recipient mail recipients. Nowhere is there a teaching of combining a multiple recipient routing list with the teaching of Walker. Everingham does not provide encryption in the delivery of the electronic routing list. Without the hindsight of the current teaching, there is no suggestion that such an escrow encryption system of the current routing list could be used and there would be no reason to combine Walker with Everingham.

For at least these reasons, the claims should be allowed over the art of record.

Claim is rejected in further view of Bouchard. Bouchard merely shows the known use of digital certificates. However, Bouchard does not cure the defects above, and therefore claim 5 should be allowable for at least the same reasons as claim 1 from which it depends.

Likewise, claims 17-20 and 36-39 and 52 should be allowable over the art of record for at least that claims 1, 29 and 45 are allowable. Geiger et al. merely show routing list rules and does not cure the defects above.

Summary

Applicants have made a diligent and bona fide effort to answer each and every ground for rejection or objection to the specification including the claims and to place the application in condition for final disposition. Reconsideration and further examination is respectfully requested, and for the foregoing reasons, Applicant respectfully submits that this application is in condition to be passed to issue and such action is earnestly solicited. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Robert N. Blackmon, Applicants' Attorney at 703-684-5633 to satisfactorily conclude the prosecution of this application.

Dated: June 5, 2006

Respectfully submitted,

Merek, Blackmon & Voorhees, LLC
673 S. Washington St.
Alexandria, Virginia 22314
Tel. 703-684-5633
Fax. 703-684-5637
E-mail: RNB@MBV-IP.com

Robert N. Blackmon
Reg. No. 39494
Attorney/Agent for Applicant(s)